

REMARKS

This Amendment is in response to the Office Action mailed November 21, 2007. Claims 1, 23 and 27 have been amended. Claim 35 has been added. Applicant respectfully requests the Examiner to reconsider the rejection and remarks made herein.

Rejection Under 35 U.S.C. § 102

A. CLAIMS 1-2 & 4-7

Claims 1-2 and 4-7 were rejected under 35 U.S.C. §103(a) as being unpatentable over Pinder (U.S. Patent No. 6,424,717) in view of Ferraro (U.S. Patent No. 5,151,782). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2D 1596 (Fed. Cir. 1988)*. Herein, the combined teachings of the cited references fail to describe or suggest all of the claim limitations.

The Office Action recited that Pinder discloses the process of a mating key generator where a key is encrypted then using this key and a second key to decrypt thereby recovering an encrypted second key in plain format. *See page 2 of the Office Action*. We disagree. As repeatedly stated, the mating key generator is a message type and Figure 2B of Pinder does not disclose the use of this message type. In the Advisory Action, the Examiner stated that “Pinder discloses the process of a mating key generator....” However, the “mating key generator” as claimed is a particular type of message – it is not a type of message generation process as alleged in the Advisory Action.

Herein, if MSK is considered to be the “key” and Kpr is construed as being the “unique key,” Pinder does not provide any discussion or suggestion that MSK *is formed from a mating key generator being a message that comprises an identifier of a supplier of the scrambled digital content, where the supplier is either a cable provider, a satellite-based provider, a terrestrial-based provider, or an Internet service provider* as claimed.

Moreover, the combined teachings of Pinder and Ferraro does not teach or suggest the limitation of the “first process block to decrypt a message using the unique key to produce a key, *the key being formed from a mating key generator that comprises an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider.*” Emphasis added. While we agree with the Examiner that Pinder does not provide such limitations, we disagree that Ferraro provides such teachings.

Column 1, lines 16-23 of Ferraro describe the use of satellites to deliver subscription programming such as HBO, where it is necessary to identify each channel (e.g., HBO) to instruction the converter box that it is authorized to descramble the programming. However, Ferraro, in combination with the teachings of Pinder, does not teach the use of the message including this HBO identifier to form the key (MSK) that was decrypted by the first process block. The mere teachings of the HBO identifier within a message does not describe or suggest the invention as claimed. We respectfully request the Examiner to reconsider these grounds for rejection.

With respect to claim 4, Applicants respectfully submit that the Office Action fails to provide any grounds for rejection. Applicants did not have the ability to address the Examiner’s rationale for the rejection because Applicants were unsure whether the ground for rejection has been overcome, as typically found when the rejection has not been restated.

As previously stated, if MSK is considered by the Examiner to be the “key” and Kpr is construed as being the “unique key” as claimed, Applicant respectfully requests the Examiner to elaborate how the key (Kpr) is formed by encrypting the mating key generator using the unique key (MSK). This limitation is explicitly stated in claim 4 and has not been addressed by the

Examiner. Applicant respectfully submits that the combined teachings of Pinder and Ferraro clearly do not describe or suggest MSK is formed by encrypting information, such as a message including the HBO identifier, using Kpr (unique key) based on the claim construction offered by the Examiner.

With respect to claims 2 and 5-7, Applicant respectfully traverses the rejection because a *prima facie* case of obviousness cannot be established for these claims. However, since claims 2 and 5-7 are dependent on claim 1, believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traverse is warranted.

Withdrawal of the §103(a) rejection as applied to claims 1-2 and 4-7 is respectfully requested.

B. CLAIMS 3 & 32

Claims 3 and 32 are rejected under 35 U.S.C. §103(a) as being unpatentable over Pinder in view of Zhang (U.S. Patent No. 6,550,008). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

First, neither Pinder nor Zhang, alone or in combination, describe or suggest that the second process block of the descrambler IC is a finite state machine. In support, the Final Office Action explicitly recites that Pinder does not disclose the descrambler IC with the second process being a finite state machine. *See pages 3& 5 of the Office Action.* We agree, but again disagree with the Examiner's contention that Zhang discloses the descrambler IC with the second process being a finite state machine. Clearly, the Examiner directed the particular support for this limitation to a single reference, Zhang. Hence, it was proper for Applicant to argue against the Zhang reference individually, in contrast with the Examiner's statements in the Advisory Action that such arguments were improper.

In the Final Office Action, the Examiner contends that column 5, lines 55-60 of Zhang provides such support, and Applicant respectfully submits that this contention is incorrect. This section (col. 5, lines 55-60) from Zhang does not provide teaching that the second process block is a finite state machine. Rather, this section describes the implementation of a controller (130)

that is placed at the head-end system (14), and hence, does not provide any suggestion for descrambling circuitry as claimed.

Second, with respect to claim 32, Applicant respectfully submits that neither Pinder nor Zhang, alone or in combination, describes or suggests a first process block that is controlled by a non-CPU based state machine to decrypt a message, namely a mating key generator, using the unique key to produce a key. The finite state machine implementation is directed to the architecture of the controller located in the head-end system and such logic does not appear to have descrambling functionality as claimed.

In light of the foregoing, Applicant respectfully requests that the Examiner withdraw the rejection of claims 3 and 32 under 35 U.S.C. §103(a).

C. CLAIMS 8 & 33

Claims 8 and 33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Pinder and in view of Alve (U.S. Patent No. 6,959,090). Applicant respectfully traverses the rejection, but since claim 8 and 33 are dependent on claims 1 and 32, believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traverse is warranted. Withdrawal of the §103(a) rejection as applied to claim 8 is respectfully requested.

D. CLAIMS 23-25 AND 27

Claim 23-25 and 27 are rejected under 35 U.S.C. §103(a) as being unpatentable over Pinder in view of Alve and Kocher (U.S. Patent No. 6,640,305). Applicant disagrees. With respect to claim 23, Applicant respectfully submits that neither Pinder, Alve nor Kocher, alone or in any combination, describes or suggests a first process block to encrypt a message using a unique, one-time programmable key to produce a first key as claimed. Applicant incorporates the arguments set forth above with respect to independent claim 1. More particularly, *the MSK, considered by the Examiner to be the first key, is not produced by encrypting a message using a unique, one-time programmable key that is considered by the Examiner to be K_{pr} . Emphasis added.*

Withdrawal of the §103(a) rejection as applied to claim 23 is respectfully requested.

With respect to claims 24-25 and 27, Applicant respectfully traverses the rejection because a *prima facie* case of obviousness cannot be established for these claims. However, since claims 24 and 25 are dependent on claim 23, believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traverse is warranted. Withdrawal of the §103(a) rejection as applied to claims 24-25 is respectfully requested.

E. CLAIM 34

With respect to claim 34, Applicant respectfully submits that this claim is in condition for allowance because claim 32 is in condition for allowance. Hence, no further discussion as to the grounds for traverse is warranted. Withdrawal of the §103(a) rejection as applied to claim 34 is respectfully requested.

Telephone Conference

Based on the foregoing and in light of the amendments to the claims, Applicant respectfully requests that the Examiner reconsider the allowability of all of the pending claims. *The Examiner is respectfully requested to contact the undersigned attorney at the phone number listed below if after reconsideration, such claims are still not in condition for allowance. This telephone conference would greatly facilitate the examination of the present application.*

Conclusion

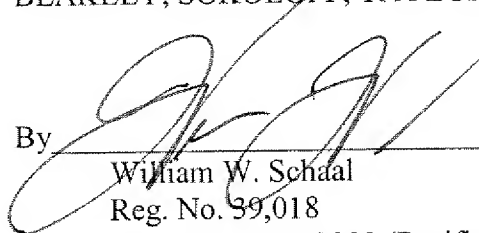
Applicant reserves all rights with respect to the applicability of the doctrine of equivalents. Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: December 27, 2007

By



William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)